Technology Law Analysis

September 07, 2017

SUPREME COURT HOLDS THAT THE RIGHT TO PRIVACY IS A FUNDAMENTAL RIGHT GUARANTEED UNDER THE CONSTITUTION OF INDIA

The technology and privacy law team of Nishith Desai Associates is presenting this analysis of the landmark Supreme Court ("**SC**") judgment of ***Justice K.S Puttaswamy (Retd.) v. Union of India and Ors***.[1] holding privacy to be a fundamental right under the Constitution of India ("**Constitution**").

While the reasoning and analysis in the judgment makes for a very interesting read for its sheer depth, in this update, we have endeavored to focus on the impact of declaring privacy as a fundamental right, the impact on private entities (non-state parties) and the potential impact on the anticipated data privacy law.

INTRODUCTION

The constitutional validity of the Aadhaar system (a nationwide biometric identification system) had been challenged before the SC. This issue was before a 5 judge bench of the Court ("**Aadhaar Bench**"). One of the key issues is whether the norms for compilation of the demographic biometric data by the government violates the right to privacy. To answer this question the SC had to first answer: whether there is a constitutionally mandated fundamental right to privacy. Due to conflicting judgments of the SC in the past, the Aadhaar Bench referred this question before a 9 judge bench of the SC ("**Privacy Bench**") to finally determine whether there existed a fundamental right to privacy. To quote the Aadhaar Bench:

"*During the course of the hearing today, it seems that it has become essential for us to determine whether there is any fundamental right of privacy under the Indian Constitution. The determination of this question would essentially entail whether the decision recorded by this Court in* ***M.P. Sharma and Ors. vs. Satish Chandra, District Magistrate, Delhi and Ors***[2] *by an eight-Judge Constitution Bench, and also, in* ***Kharak Singh vs. The State of U.P. and Ors.***[3] *by a six-Judge Constitution Bench, that there is no such fundamental right, is the correct expression of the constitutional position.* ***(emphasis as per Court order)"***

The Privacy Bench unanimously held that the right to privacy is fundamental right protected under the Constitution. The judges have delivered 6 judgments: Justice Chandrachud has written on behalf of himself, Chief Justice JS Khehar, Justice Agrawal and Justice Abdul Nazeer ("**Lead Judgment**"). Justice Chelameshwar, Justice Bobde, Justice Sapre, Justice Nariman and Justice Kaul have written separate judgments providing their own findings, conclusions and observations (referred to as "**Single Judge Judgment(s)**"). A consolidated order ("**Order**") holds that:

i. The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution; and

ii. The earlier judgments of the SC in Kharak Singh and MP Sharma to the extent they held otherwise, are overruled.

The judgments in total run into 547 pages. The judgments trace the history of Indian constitution, development of jurisprudence with respect to fundamental rights through various SC cases, examine scholastic articles, foreign jurisprudence and case laws and of course international treaties.

The Lead Judgment starts by acknowledging that (i) Privacy allows each individual / person to be left alone in a core which is inviolable; (ii) this autonomy is conditioned by their relationships with the rest of society; (iii) those relationships pose questions to autonomy and free choice. The overarching presence of state and non-state entities regulates aspects of social existence which bear upon the freedom of the individual; and (iv) privacy is required to be analyzed in an interconnected world and the SC has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world. The Single Judge Judgments also refer to digital economy and non-state parties' role. These observations are discussed in detail later.

Though the Lead Judgment and Single Judge Judgments reach the same conclusion, each judgment deals with arguments of the petitioner and the state separately and at times in slightly different manner. Hence, an in depth analysis may be required of different aspects to arrive at the binding ratio. Some aspects dealt with in Single Judge Judgments may not be dealt with in the Lead Judgment or may not be dealt with in equal detail. In such cases, the binding nature of such aspect will have to be analyzed further.

Further, all earlier cases that deal with the fundamental rights, its ambit and principles on which restrain may be applied to its exercise will be applicable with respect to privacy as a fundamental right. Hence, in subsequent cases when state action is challenged on the ground of privacy, in addition to the present case, such earlier cases may also

Research Papers

Mergers & Acquisitions
July 11, 2025

New Age of Franchising
June 20, 2025

Life Sciences 2025
June 11, 2025

Research Articles

2025 Watchlist: Life Sciences Sector India
April 04, 2025

Re-Evaluating Press Note 3 Of 2020: Should India's Land Borders Still Define Foreign Investment Boundaries?
February 04, 2025

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals
January 15, 2025

Audio

CCI's Deal Value Test
February 22, 2025

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Reimagining CSR: From Grant Giving to Blended Finance & Outcome Based Funding
June 16, 2025

Courts vs Bankruptcy code: The

come to aid.

I. WHAT WAS THE POSITION OF 'PRIVACY' AS A FUNDAMENTAL RIGHT EARLIER?

The Judgment has not created a new right to privacy as a fundamental right but has clarified the status of the right to privacy as fundamental right under the Constitution. It traced its recognition in the right to life and personal liberty under Article 21 of the Constitution of India ("**Constitution**"), but found that it was also footed in certain other rights, such as Article 19[4].

The judgment clarifies that a constitutional right to privacy can be defined in both negative and positive terms, i.e:

- To protect the individual from unwanted intrusion into their private life, including sexuality, religion, political affiliation, etc. (the negative freedom)
- To oblige the state to adopt suitable measures to protect an individual's privacy, by removing obstacles to it (the positive freedom)

The SC's ruling is rooted, *inter alia*, in the following reasoning:

i. **Privacy as an inalienable right**: Privacy is a natural right, inherent to a human being. It is thus a pre-constitutional right which vests in humans by virtue of the fact that they are human. The right has been preserved and recognized by the Constitution, not created by it. Privacy is not bestowed upon an individual by the state, nor capable of being taken away by it. It is thus inalienable.

ii. **Relationship with Dignity**: It was argued by the state that the recognition of privacy would require a Constitutional amendment, and could not be 'interpreted' into the Constitution. The judgment has recognized that privacy was intrinsic to other liberties guaranteed as fundamental rights under the Constitution. Privacy is an element of human dignity, and ensures that a human being can lead a life of dignity by, among other things, exercising a right to make essential choices, to express oneself, dissent, etc. Dignity was, consequently, an intrinsic aspect of the right to life and liberty enshrined under Article 21 of the Constitution, as 'life' was not limited to mere existence, but was made worth living because of the attendant freedom of dignity. It was only when life could be lived with dignity that liberty could be of any substance.

iii. **Commitment to International Obligations**: The recognition of privacy as fundamental constitutional value was a part of India's commitment[5] to safeguard human rights under international law under the International Covenant of Civil and Political Rights ("**ICCPR**") which found reference in domestic law under the Protection of Human Rights Act, 1993. The ICCPR recognizes a right to privacy[6]. The Universal Declaration of Human Rights too specifically recognizes a right to privacy.[7]The Judgment has held that constitutional provisions had to be read and interpreted in a manner such that they were in conformity with international commitments made by India.

II. WHAT ARE THE SPECIFIC FACETS OF PRIVACY THAT HAVE BEEN REFERRED TO BY THE COURT?

The submission of the government was that the SC cannot recognize a juristic concept which is so vague and uncertain that it fails to withstand constitutional scrutiny. The judgments rejected this argument. In the simplest form, the judgments recognize the right as "*right to be let alone*". Justice Nariman categorizes the right as having three aspects: personal privacy (such as the right to move freely), informational privacy and the privacy of choice.

The SC has traced the history of recognition of various facets of the right to privacy by citing various scholastic writing, .Indian and foreign judgments and provides description of privacy right. However, the Lead Judgment succinctly concludes that:

"This Court has not embarked upon an exhaustive enumeration or a catalogue of entitlements or interests comprised in the right to privacy. The Constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the rule of law. The meaning of the Constitution cannot be frozen on the perspectives present when it was adopted. Technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present. Hence the interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its content bearing in mind its basic or essential features.'

Justice Bobde has stated that scope and ambit of a constitutional protection of privacy can only be revealed on a case-by-case basis.

In this context, the Lead Judgment relies on an article that represents privacy through a diagrammatic structure[8] that identifies nine types of privacy:

- Bodily privacy: Privacy of the physical body against violations and restraints of bodily movement
- Spacial Privacy: Privacy of a space, such as family life and intimate relations
- Communicational Privacy: Right against access to communication, or control over it
- Proprietary Privacy: Right to use property as a means to shield facts or information
- Intellectual Privacy: Privacy of thought, mind, opinions and beliefs
- Decisional Privacy: The ability to make intimate decisions
- Associational Privacy: Privacy of the choice of who to interact with
- Behavioral Privacy: The ability to control the extent of access even while conducting publically visible activities
- Informational Privacy: An interest in preventing information about the self from being dissemination, and controlling the extent of access to the information

However, it is important to examine each judgment to have an illustrative list of rights enumerated by the SC so that while framing any law or taking any action, the government has enough guidance on whether such law or action is likely to violate the right to privacy.

III. WHAT IS THE IMPACT OF DECLARING PRIVACY AS A FUNDAMENTAL RIGHT? WHAT IS THE IMPACT OF THE JUDGMENT ON NON-STATE PARTIES ?

JSW-Bhushan Saga
June 04, 2025

Vyapak Desai speaking on the danger of deepfakes | Legally Speaking with Tarun Nangia | NewsX
April 01, 2025

The impact of recognizing privacy as a fundamental right, as opposed to a statutory or a common-law right, is that it is an inviolable right. A fundamental right provides a touchstone on which the validity of a law may be determined or a state's action may be assessed. While a statutory right may be modified, amended, or annulled by a simple act of legislation, a constitutional right is not subject to amendment or annulment at the instance of the legislature. Any abridgment of a constitutional right, must meet the tests prescribed under Article 21, Article 19, or the specific freedom it seeks to abridge. The impact of the Order is already apparent. In a recent case Delhi High Court has raised a question whether private blackberry messenger messages can be relied upon by the state to impugn a criminal offence against the person, in view of the privacy ruling of the SC[9].

To clarify, fundamental rights under Article 19 and 21 are as such enforceable only against the state or instrumentalities of the state and not against non-state parties. However, almost all the 6 judgments highlight the need for data protection law to control actions of the non-state parties as well. The horizontal application of the right to privacy will have to be tested in the view of this judgment. In fact the Lead Judgment calls upon the government to bring out a detailed data protection regime based on the broad guidelines laid down in the judgments. Most of the views are expressed in this connection – referred to as 'informational privacy' in the Judgment – are discussed in detail below in section VIII.

At present as against the non-state entities, privacy is recognized as a common law (as opposed to a constitutional) right. The enforcement will depend on facts and circumstances of the case. Under the Information Technology Act, 2000 and rules framed thereunder there are limited provisions with respect to protection of personal information and sensitive data and personal information.

IV. WHAT ARE THE REASONABLE RESTRICTIONS ON THE FUNDAMENTAL RIGHT TO PRIVACY THAT HAVE BEEN RECOGNIZED BY THE COURT?

Since the fundamental rights are not to be read in a silo, any infringement of fundamental rights will therefore have to pass the basic tests of Articles 21 and 14 of the Constitution. These tests are[10]:

1. The need for an existence of a law; and
2. The law should not be arbitrary; and
3. The infringement of the right by such law should be proportional for achieving a legitimate state aim.

The judgments have recognized the below mentioned restrictions on the right to privacy

- The Lead Judgement notes the tests for the reasonable restrictions on the right to privacy in Para 3 (H) of the conclusion. It holds that a law which encroaches upon the right to privacy will have to *"withstand the touchstone of permissible restrictions on fundamental rights*" Any infringement of privacy must be by a law which is "*fair, just and reasonable"*. The three-fold requirement for such infringement would be: "*(i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them*"
- Justice Chelameshwar has held in paragraph 45 of his judgment that aside from meeting the 'fair, just and reasonable' requirement under Article 21, there should be a requirement for 'compelling state interest' for those privacy claims which deserve the 'strictest scrutiny'
- Justice Bobde, in paragraph 45 of his judgment held that any infringement of the fundamental right to Privacy must pass the same standard required for the infringement of personal liberty, ie. In terms of the judgement in the case of ***Maneka Gandhi v. Union of India***[11], such law must be "*fair, just and reasonable, not fanciful, oppressive or arbitrary"*
- Justice Nariman has held in paragraph 60 of his judgement that statutory restrictions on privacy would prevail if it is found that the 'social or public interest and the reasonableness of the restrictions outweighs the particular aspect of privacy claimed.
- Justice Sapre in paragraph 26 of his judgment says that the right to privacy is subject to reasonable restrictions "in view of the social, moral and compelling public interest that the state is entitled to impose by law."
- Justice Kaul has held in paragraph 72 of his judgment that that right to privacy would be subject to reasonable restrictions on the grounds of national security, public interest and the grounds enumerated in the provisos to Article 19 of the Constitution.

V. CAN FUNDAMENTAL RIGHTS BE WAIVED BY CONSENT?

The state argued that privacy cannot be held to be a fundamental right, as fundamental right cannot be waived. This would lead to several complications arising with regard to the functioning of the state. This argument was made on the basis that the state would be virtually barred even from contractually collecting any information from individuals in India and this would hamper the functioning of the state as it is required to collect certain information of citizens while exercising its required functions.

Interestingly, the Lead Judgement does not deal with this argument of the government. It merely refers to SC judgment "***Behram Khurshed Pesikaka v. State of Bombay***"[12] and concurred with the view that "*Part III of the Constitution is a part of the wider notion of securing the vision of justice of and, as a matter of doctrine, the rights guaranteed were held not to be capable of being waived*"[13].

In this regard Justice Nariman in his judgment has observed[14] as follows:

- *Statutory provisions that deal with aspects of privacy would continue to be tested on the ground that they would violate the fundamental right to privacy, and would not be struck down, if it is found on a balancing test that the social or public interest and the reasonableness of the restrictions would outweigh the particular aspect of privacy claimed. If this is so, then statutes which would enable the State to contractually obtain information about persons would pass muster in given circumstances, provided they safeguard the individual right to privacy as well……*
- *…. in pursuance of a statutory requirement, if certain details need to be given for the concerned statutory purpose, then such details would certainly affect the right to privacy, but would on a balance, pass muster as the State action*

concerned has sufficient inbuilt safeguards to protect this right – viz. the fact that such information cannot be disseminated to anyone else, save on compelling grounds of public interest.

Thus, the threshold for state collecting the data from the citizens and the purpose for which it will be used is stringent. The same threshold in our view however should not apply when the non-state parties collect and use data.

A question may be raised about, when the state acts in a commercial capacity, whether fundamental rights may still be enforced against the state and whether the same threshold for consent as discussed above will apply in relation to such commercial activity. In this connection, several earlier case laws have clarified that executive action (as stated below), will have to satisfy the test of Article 14 of the Constitution, irrespective of whether the function being exercised by the state in its capacity as a sovereign or in a commercial capacity or in any other capacity. This viewpoint was upheld by the Court in ***Air India Ltd. vs. Cochin International Airport Ltd***[15] and ***Ramana Dayaram Shetty vs. International Airport Authority of India and Ors***.[16].

In light of the above, it may be argued that there is a duty imposed on the state to act reasonably while obtaining consent from individuals for the collection of information which falls under the protections envisaged under the right to privacy, without regard to under what capacity function is being exercised by the state.

VI. WHAT IS THE POTENTIAL IMPACT OF THE JUDGEMENT ON AADHAAR AND WHAT REFERENCES HAVE BEEN MADE IN THE JUDGEMENT WHICH MAY HAVE AN IMPACT ON THE AADHAAR JUDGEMENT?

While the judgment itself does not seek to (and was not intended) to answer the constitutional challenge to The Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits And Services) Act, 2016 ("**Aadhaar Act**"), the judgments will have bearing on Aadhaar ruling. The Aadhaar Act will have to satisfy the three pronged test as discussed above, since under the Aadhaar Act personal information such as biometric information is collected and processed by the government. Other than Aadhaar Act itself, the manner in which the use of Aadhaar Card is being mandated by the government for various purposes, will also need to be tested on the basis of the privacy judgment.

In the context of this evaluation, it is imperative to note that the Aadhaar scheme which was first introduced as a means of targeted distribution of subsidies, is today being implemented towards a variety of purposes, including the fight against black money, transaction authentication, and 'know your customer' requirements for banks and telecom companies. Aspects of Aadhaar Act, such as (i) security of the Aadhaar system, (ii) the inability of the individual to file complaints (for violation under the Aadhaar Act) relating to theft or misuse of their data[17], and (iii) the inability to withdraw / delete one's data once registered with the UIDAI, will also likely come under scrutiny.

The following observations of the court in the judgment throw light on some of the questions surrounding the Aadhaar challenge. *First*, while the court rejected the argument that furtherance of welfare objectives should take precedence over right to privacy[18], it has indicated that the fulfillment of welfare objectives would be a legitimate aim towards which the right to privacy could be infringed (provided the other conditions of a reasonable restriction are met).[19] *Secondly*, the primacy of individual consent (in relation to one's data / information) as highlighted by the Court[20], provides possible context to the discussion on the mandatory and permanent nature of the Aadhaar.

We will soon publish our detailed analysis on the Aadhaar Act and Aadhaar scheme in the light of this judgment.

VII. WHAT WOULD BE THE REASONABLE EXPECTATION OF PRIVACY, ESPECIALLY IN A PUBLIC PLACE?

The Lead Judgment in its conclusion summarizes this aspect[21] as follows:

"While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being."

The SC has not however, gone on to examine or analyze the extent or scope of the legitimate expectation of privacy of an individual in a public place as such an examination / determination would differ based on the facts of each matter at hand. The aforementioned determination is additionally relevant in light of several instances wherein certain actions have been question to be in violation of the right to privacy of individuals in public such as the installation of CCTV cameras by the government in public areas. It may be argued that now the installation of the CCTV cameras by the government needs to satisfy the test of reasonable restriction as discussed above.

Justice Bobde has negated the argument of State of Gujarat that only those privacy claims which involve a 'reasonable expectation of privacy' be recognized as protected by the fundamental right. He goes on to explain

Such a formulation would exclude three recurring red herrings in the Respondents' arguments before us. Firstly, it would not admit of arguments that privacy is limited to property or places. So, for example, taking one or more persons aside to converse at a whisper even in a public place would clearly signal a claim to privacy, just as broadcasting one's words by a loudspeaker would signal the opposite intent. Secondly, this formulation would not reduce privacy to solitude. Reserving the rights to admission at a large gathering place, such as a cinema hall or club, would signal a claim to privacy. Finally, neither would such a formulation require us to hold that private information must be information that is inaccessible to all others.

Justice Nariman has also discussed the state's argument on the "reasonable expectation of privacy test", which provides that, "if information is voluntarily parted with by an individual, no right to privacy exists", as was laid down in ***Katz v. United States***[22] . Justice Nariman has rejected the state's argument that the Court should follow the "reasonable expectation of privacy test", while determining the contours of the right to privacy by referring to the judgment of the SC in ***District Registrar and Collector, Hyderabad & Anr. v. Canara Bank, etc***.[23], and thereby holding that that the "reasonable expectation of privacy test" has no plausible foundation under Article's 14, 19, 20 and 21 of the Constitution of India.

VIII. DATA PROTECTION OR 'INFORMATIONAL PRIVACY'

The Judgments at several places deal with informational privacy (especially in the context of inter-connected digital world), both in the hands of state and non-state entities.

Some Judgments discuss various aspects of collection, use and handling of data e.g. big data, data analytics, use of wearable devices and social media networks resulting in generation of vast amounts of user data relating to end users' lifestyles, choices and preferences, use of cookies files on browsers for tracking user behavior and for the creation of user profiles.

The Lead Judgment specifically deals with informational privacy but substantial part of the discussion is on the handling of information by the State. The Lead Judgment contemplates a robust regime (as per requirements of Article 21) satisfying the tests below:

- existence of law to justify an encroachment on privacy; and
- the requirement of a need, in terms of a **legitimate state aim**, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action. [The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits]; and
- the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law.

The Lead Judgment relied upon SC judgment in the matter of *District Registrar and Collector, Hyderabad v Canara Bank*[24] in relation to the informational privacy in the hands of the nationalized Bank. Some Judgments also refer to the recommendations made by the Expert Group's Report set up earlier by the government in 2012, proposing a framework for the protection of privacy concerns in India[25]. However, no binding observations have been made by the SC with respect to the recommendations made by the Expert Group.[26]

In the conclusion of the Lead Judgment the SC acknowledges that the government has set up committee under Justice B N Srikrishna ("**MeiTy Committee**") for suggesting appropriate data protection law in India and directs that the matter shall be dealt with appropriately by the Union government having due regard to what has been set out in its judgment.[27]

Some judgments have alluded to different facets of data protection regime. Most of them appear more as discussion points rather than binding ratio. The Lead Judgment refers to non-discriminatory treatment on the basis of data collected. Justice Kaul has alluded to the need for "right to be forgotten". He has also suggested that EU law may be a useful guidance.

Justice Kaul suggests that profiling of individuals by the State that leads to discrimination is not acceptable however, such profiling can be used for public interest and protection of national security. He deals with the right to control information in some detail and observes as follows. The following observations are not specifically distinguished as whether they apply in relation to state and/or non-state.

- *from the right to privacy in this modern age emanate certain other rights such as the right of individuals to exclusively commercially exploit their identity and personal information, to control the information that is available about them on the 'world wide web' and to disseminate certain personal information for limited purposes alone;*
- *There is no justification for making all truthful information available to the public. The public does not have an interest in knowing all information that is true. Which celebrity has had sexual relationships with whom might be of interest to the public but has no element of public interest and may therefore be a breach of privacy. Thus, truthful information that breaches privacy may also require protection.*
- *This also means that an individual may be permitted to prevent others from using his image, name and other aspects of his/her personal life and identity for commercial purposes without his/her consent.*

The impact of abovementioned observations in relation to right of celebrities will need to be examined in detail

Justice Kaul further discusses the right to control and correct information on the world wide web and alludes to right to be forgotten as essential ingredient subject to some limitations.

The three tests specified above that apply in relation to a fundamental right, should not necessarily apply in relation to handling of the data by non-state parties. If the same three tests were to be made applicable to non-State then the data protection regime will be very restrictive and will thwart innovation and efficient delivery of goods and services. Therefore, the proposed data protection regime ought to make distinction between the handling of the data by the State and Non-State parties.

Justice Kaul has specifically dealt with privacy concerns against non-state parties, and some of the key observations are below:

- *A large number of people would like to keep such search history private, but it rarely remains private, and is collected, sold and analysed for purposes such as targeted advertising. Of course, 'big data' can also be used to further public interest. There may be cases where collection and processing of big data is legitimate and proportionate, despite being invasive of privacy otherwise.*
- *Knowledge about a person gives a power over that person. The personal data collected is capable of effecting representations, influencing decision making processes and shaping behaviour. It can be used as a tool to exercise control over us like the 'big brother' State exercised. This can have a stultifying effect on the expression of dissent and difference of opinion, which no democracy can afford.*
- *There is an unprecedented need for regulation regarding the extent to which such information can be stored, processed and used by non-state parties. There is also a need for protection of such information from the State. Our Government was successful in compelling Blackberry to give to it the ability to intercept data sent over Blackberry devices. While such interception may be desirable and permissible in order to ensure national security, it cannot be unregulated.*

One way to view the question of how the fundamental right to privacy affects non-state parties is to see the judgment

as requiring (or, at the least, suggesting) that the State create a data protection law.[28] This is to preserve citizens' informational privacy (or per Justice Nariman, their privacy interest of "data protection")[29] against non-State parties. In the past, similarly, the SC observed the need for a law against sexual harassment in the workplace, and directed the government to frame such a law in the interest of protecting fundamental rights (*Vishaka v. State of Rajasthan*)[30].

IX. WAY FORWARD

Justice Kaul has stated in Para 70 of his opinion that:

"The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed"

This assertion has been supported by an observation by Justice Chandrachud in Para 177 of the Lead Judgement[31]. Read together, it appears that the need for 'consent' in the data protection regime will be one that is constitutionally mandated as part of the right to privacy.

Considering the observation in the Lead Judgment and by Justice Kaul with respect to consent and the discussion regarding the AP Shah Committee, it is likely that the data protection law will contain the following broad aspects:

1. It is likely to technologically neutral,
2. While the present regime only makes the data controller accountable for 'Sensitive Personal Data or Information', it is expected that this regime will be expanded to include a wider gamut of data.
3. It is likely to expand the scope of the consent requirements and permissions for data sharing.

Further:

- Several legislations such as Aadhaar Act under which the personal information is collected by the central and state government will have to pass the tests laid down by the SC.
- State actions that deal with privacy and personal information will be tested on the reasonable restriction principles stated above. E.g. the Delhi High Court has already questioned reliance on BBMs of the individual in a criminal case against him.
- In the WhatsApp and Facebook case, the courts will have to determine whether WhatsApp's revised terms and conditions to share certain data with Facebook violate the users' inherent right to privacy and confidentiality in line with the petitioners' arguments that WhatsApp is performing a 'public duty' and is subject to the obligations of telecom service providers in re. wiretapping etc. If the SC does rule so, then it is likely to apply the principles of privacy enunciated in this judgment. If the court holds otherwise then it seems the fate may be determined only by review of contractual relationship between the parties. In such a case, it would be a civil remedy rather than a writ remedy. It is also likely that the SC as part of this verdict is also going to rule on the form and manner in which consent must be taken from users in the digital domain.
- Following the judgment of the Privacy Bench, another public interest litigation has been clubbed along with the WhatsApp and Facebook case which challenges the constitutional validity of the existing data protection framework, i.e. the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Data Protection Rules**"). This challenge has been made on grounds of lack of adequate remedy for Indian citizens against foreign entities such as Facebook, Twitter and Google whose Indian subsidiaries do not have any control over data. Whilst denying the petitioners request for an immediate interim injunction the SC has nevertheless issued notices to WhatsApp, Twitter and Google to respond within 4 (four) weeks to regarding their policies on disclosure of data to third parties, following which it will evaluate any request for interim orders.
- Much depends on the anticipated data protection law to be introduced by the government. The government in its last submission before the SC in the WhatsApp case has also alluded to the fact that following the report of the MeiTy Committee they will consider bringing a law on data protection. The MeiTy Committee while preparing its observations will have to take into account the ruling of the Privacy Bench. In doing so, the MeiTy Committee will have to evaluate whether a single data protection framework will apply to state and non-state entities or whether the thresholds ought to be different and therefore different set of provisions should apply.

---

[1] WP (C) 494 of 2012
[2] *1950 SCR 1077*
[3] *1962 (1) SCR 332*
[4] Article 19 of Constitution of India: Protection of certain rights regarding freedom of speech etc.
[5] Article 51 of the Constitution, which forms part of the Directive Principles mandates that India foster respect for international law and its treaty obligations
[6] Article 17 of the ICCPR states: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation 2. Everyone has the right to the protection of the law against such interference or attacks.
[7] Article 12, Universal Declaration of Human Rights
[8] Paragraph 141, Part L of the Lead Judgment
[9] http://www.thehindu.com/news/cities/Delhi/can-bbm-message-be-read-as-proof-after-privacy-verdict-asks-hc/article19590467.ece
[10] Paragraph 180 of the Lead Judgment and Paragraph 3(H) of the Lead Judgment's conclusion
[11] 1978 SCR (2) 621
[12] (1955) 1 SCR 613
[13] Paragraph 112 of the Lead Judgment
[14] Paragraph 60 of Justice Nariman's judgment
[15] (2000) 2 SCC 617
[16] (1979) 3 SCC 489
[17] See Section 47, the Aadhaar Act;
[18] Paragraph 154-155 of the Lead Judgment, Paragraph 45 of Justice Nariman's judgment
[19] Paragraph 154-155 of the Lead Judgment..
[20] .Paragraph 176 of the Lead Judgment.
[21] Paragraph 3 (F) of the Conclusion of the Lead Judgment.
[22] 389 U.S. 347 (1967)

[23] (2005) 1 SCC 496

[24] (2005) 1 SCC 496

[25] The framework was based on five salient features (i) technological neutrality and interoperability with international standards; (ii) multi-dimensional privacy; (iii) horizontal applicability to state and non-state entities; (iv)conformity with privacy principles; and (v) a co-regulatory enforcement regime. The Expert Committee proposed nine privacy principles, namely notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security and openness, and accountability.

[26] Report of the Expert Group available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[27] The Ministry for Electronics and Information Technology ("MeitY") has constituted a committee of experts, in July, 2017, under the chairmanship of Justice B.N Srikrishna, in order to identify key data protection issues in India, recommend methods of addressing such issues and to prepare a draft data protection bill.

[28] E.g., Paragraph 5 of the conclusion of the Lead Judgement.

[29] Paragraph 46 of Justice Nariman's opinion.

[30] (1997) 6 SCC 241

[31] *"The sphere of privacy stretches at one end to those intimate matters to which a reasonable expectation of privacy may attach. It expresses a right to be left alone. A broader connotation which has emerged in academic literature of a comparatively recent origin is related to the protection of one's identity. Data protection relates closely with the latter sphere. Data such as medical information would be a category to which a reasonable expectation of privacy attaches. There may be other data which falls outside the reasonable expectation paradigm. Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual. This is evident from the emphasis in the European data protection regime on the centrality of consent. Related to the issue of consent is the requirement of transparency which requires a disclosure by the data recipient of information pertaining to data transfer and use"*